DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES		
Reference: 06-03	**Effective Date: March 18, 1996**	**Page: 1 of 2**
SUBJECT: INFORMATION TECHNOLOGY ASSET SECURITY POLICY		
RATIONALE: **Computer system resources and information of the Department of Human Services are information technology assets of the State of Utah and must be protected. This includes protection from unauthorized disclosure, modification, or destruction, whether accidental or intentional.**		

INFORMATION TECHNOLOGY ASSET POLICY

DHS Computer Security Policy Statement

Managers, employees, or users of information technology assets are subject to all requirements and sanctions of State statute and administrative rules. Policies and procedures regarding proper use, ethics and conduct while using information technology assets either purchased or developed must also be followed.

Proper use is defined as employees, contractors, and volunteers being responsible to see that a State information technology asset is used in an effective, ethical and lawful manner.

Users of electronic mail, voice mail, and facsimile, as applicable, must be aware that they are nonconfidential means of electronic messaging and/or document exchange for government related use and subject to monitoring. Brief personal messages to coworkers will be allowed; as long as these messages are not too excessive, do not interfere with the normal conduct of business, do not involve solicitation, do not involve a for-profit personal business activity or have the potential to embarrass the state agency. Users must be aware of the value and sensitivity of the information they are sending and may need to select a more conventional method of delivery.

DHS employees may maintain additional commercial software on their workstation, i.e., local disk drives or other writeable media, if the software supports a government related function. The software must also be in compliance with all licensing and copyright laws and the employee must retain documentation to identify ownership.

Each employee is encouraged to review Administrative Rules R365-3 and R365-4 for further information. Copies can be obtained from the Bureau of Information Technology, Security Group.

Access to State information is given on a need to know basis and can only be authorized by certified owners of the specific information. Unauthorized or improper access of networks, files or software, or providing access to others by disclosing access codes or passwords will be grounds for disciplinary action and/or termination in accordance with the Utah Administrative Code, Section R477-11

Compliance and Responsibilities

DHS intends to comply with the terms and conditions of all software licensing agreements and copyright laws. Reasonable methods are to be used in all DHS locations to protect information technology assets from piracy, damage, improper or illegal use, that results in Department loss, liability, or loss of productivity. Compliance and responsibilities include the following:

A. D/I/O/R/B Directors are responsible in each of their agencies for compliance with this policy. Actual monitoring, inventory and retention of ownership documentation for all information technology assets, and commercial software may be delegated to staff.

B. DHS shall acquire, use and copy proprietary software in accordance with licensing agreements. If an agency wishes to use the secondary copy authorization granted by some vendor licenses, the agency is responsible for developing a procedure that adheres to all license provisions.

C. Proprietary and public domain software must be approved and tested by the Bureau of Information Technology (BIT) prior to use on any Department owned local area network. The Director of BIT may delegate this authority.

D. Where software is used by a DHS employee on a local workstation without BIT testing and/or approval, the employee may be liable for any damages resulting from improper use. The software must also be in compliance with all licensing and copyright laws and the employee must retain documentation to identify ownership.

E. DHS may retain the right, title, and interest in any employee or contractor developed software. All development contracts should clearly define ownership of the software and documentation developed (refer to Administrative Rule R365-3.)

F. Non-business related use of all Department owned equipment, software, and data must be used in accordance with Administrative Rule R365-4.

G. All DHS owned data or software must be removed from the storage media of any computer hardware device before disposition or transfer of equipment, unless software and documentation is included as part of the transfer.

H. Employees not in compliance with this policy are subject to disciplinary action and/or termination in accordance with the Utah Administrative Code, Section R477-11.

I. Compliance with this policy is subject to review by State and Federal auditing agencies.

Robin Arnold-Williams DATE: 03-18-96

Robin Arnold-Williams, Executive Director
Department of Human Services